SAMPLED NETFLOW

Ruchi Kapoor
Angelo Calabrese
Rakesh Dubey
Charles Goldberg

A new network traffic data collection technique is presented. A group of information is received, and a determination is made whether to process the group of information for network data collection according to a sample mode and a sample rate. If the determination is to process the group of information, the group of information is processed for network data collection. The group of information is forwarded according to its destination address. The group of information can be an IP packet and the sample mode can be, for example, one of linear, exponential, natural log, burst and traffic attribute. To process the group of information, a determination is made whether the group of information is part of one or more recorded traffic flows. If not, a new entry in a table is created. If so, a field in an existing entry in the table is incremented. In addition, a traffic information packet is created and transmitted to a network traffic data collection application. The traffic information packet can consist of a header and one or more flow records.